Cassandra Crossing/ Obama, la Cina, le app

(341) —Gli USA e la Cina temono reciprocamente le rispettive cimici. Un ordinario cittadino dovrebbe fidarsi solo perché hardware e…

Cassandra Crossing/ Obama, la Cina, le app
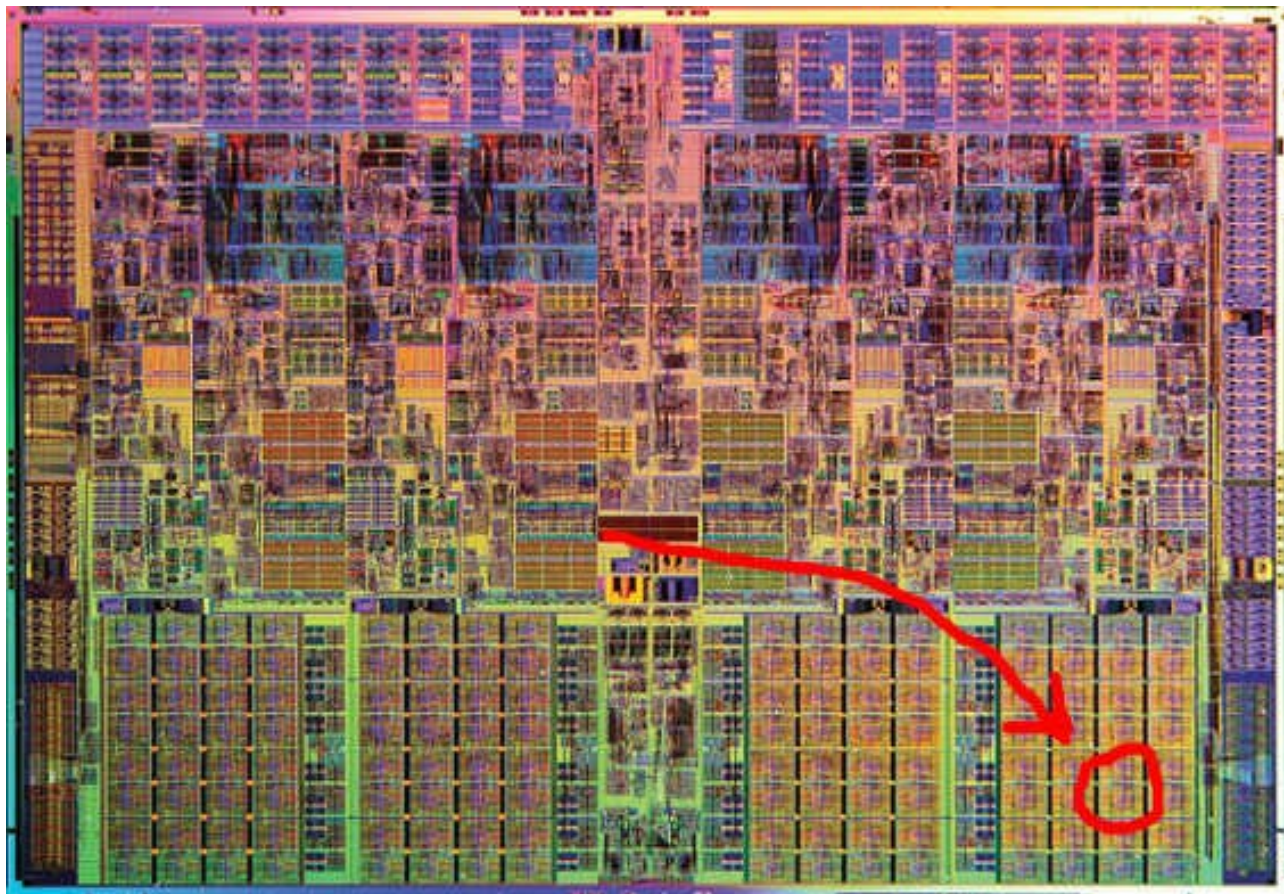
Figure 1:

(341)—Gli USA e la Cina temono reciprocamente le rispettive cimici. Un ordinario cittadino dovrebbe fidarsi solo perché hardware e software dichiarano trasparenza e innocuità? Non solo l'Internet delle Cose, ma anche le Cose di Internet possono essere pericolose.

20 marzo 2015— L'altro giorno, vittima di un momento di sbandamento, ho provato ad installare su mio smartphone la mia prima app commerciale, quella di Twitter, da un repository che sapevo pericoloso come Play Store, invece che da un più sicuro F-Droid.

Infatti, come molti dei 24 implacabili lettori già sanno, il dumbphone di Cassandra è defunto per cadute e consunzione, e la sua tasca è stata nuovamente occupata da un normale smartphone di generazione n-2 (quindi molto economico), debitamente ed accuratamente (per quanto possibile) disinfestato da qualsiasi cosa non fosse indispensabile e con tutte le autorizzazioni accuratamente negate.
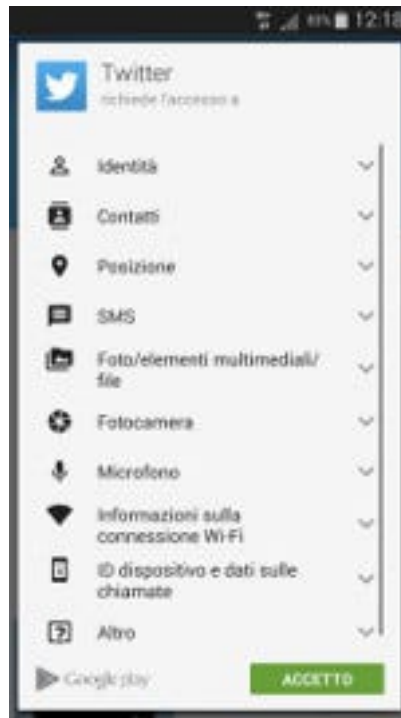
Figure 2:

Lo so, è stato un momento di debolezza, ma la schermata di richiesta di autorizzazioni che mi è comparsa davanti mi ha traumaticamente riportato alla realtà, alla necessità di non cedere alle comodità. e mi ha fatto tornare sui miei passi. Non succederà più.

In particolare mi ha disgustato l'ultima voce dell'elenco che, dopo aver chiesto di sapere tutto, ma proprio tutto, voleva anche sapere "altro".

Continuerò quindi ad ascoltare e saltuariamente fare qualche cinguettio esclusivamente da browser, onde evitare di avere troppi curiosi in mezzo ai miei dati.

E' strano, ma recentemente il presidente Obama si è trovato in una situazione simile, cioè a ribadire la sua preoccupazione nel trovarsi ad essere spiato dai suoi aggeggi elettronici.

Ha infatti minacciato anatemi commerciali alla Cina se il governo cinese avesse preteso (continuato?) ad inserire backdoor nell'elettronica colà prodotta (quasi tutta ormai).

Bizzarro, perché anche in questo il governo che ora il presidente Obama incarna era stato un precursore; già negli anni '90, tentò di imporre l'inserimento in tutti gli apparecchi telefonici di un chip denominato MYK-78, ma meglio noto come Clipper chip, che permettesse le "intercettazioni di stato" di qualsiasi telefonata, anche criptata.

In questo i predecessori di Obama sono stati fermati, ma come il Datagate ha dimostrato al di là di ogni ragionevole dubbio, altre strade ben più potenti per un tecnocontrollo globale sono state percorse con grande successo dagli Stati Uniti, e certamente anche da altre nazioni.

E che queste attività dell'intelligence degli Stati Uniti fossero note a chi doveva saperlo è dimostrato anche dalla minaccia uguale e contraria che il governo cinese inviò anni fa a quello statunitense temendo (per usare un eufemismo) la fornitura di apparati high-tech e software messi al soldo dell'NSA; la preoccupazione era tale da spingerlo a far produrre alternative hardware e software di produzione nazionale e garantiti a prova di spioni.

Per farla breve, Obama, il governo cinese e Cassandra hanno problemi simili, anche se su scale

molto diverse. Tutti e tre hanno bisogno di aggeggi ed applicazioni high-tech ma ne temono, ed a ragione, le non possibili ma sicure conseguenze.

Ormai non basta più utilizzare software, e magari firmware liberi. Una scheda di rete può avere un firmware inquinato da malware, come nel caso di Rakshasa.

Un hard disk puo ospitare al suo interno un intero sistema operativo invisibile che resiste anche alla formattazione e non occupa la cpu del computer.

Tutte queste cose sono state scoperte da hacker, e se non prima, certamente dopo sono finite nella faretra di organizzazioni di intelligence e governi.

Obama non è preoccupato solo per questo, ma sta probabilmente pensando a silicio disonesto. Cosa fa l'ultimo gruppo di transistor in basso a destra in questo chip i7?

E' quel rettangolino indicato dalla freccia rossa.
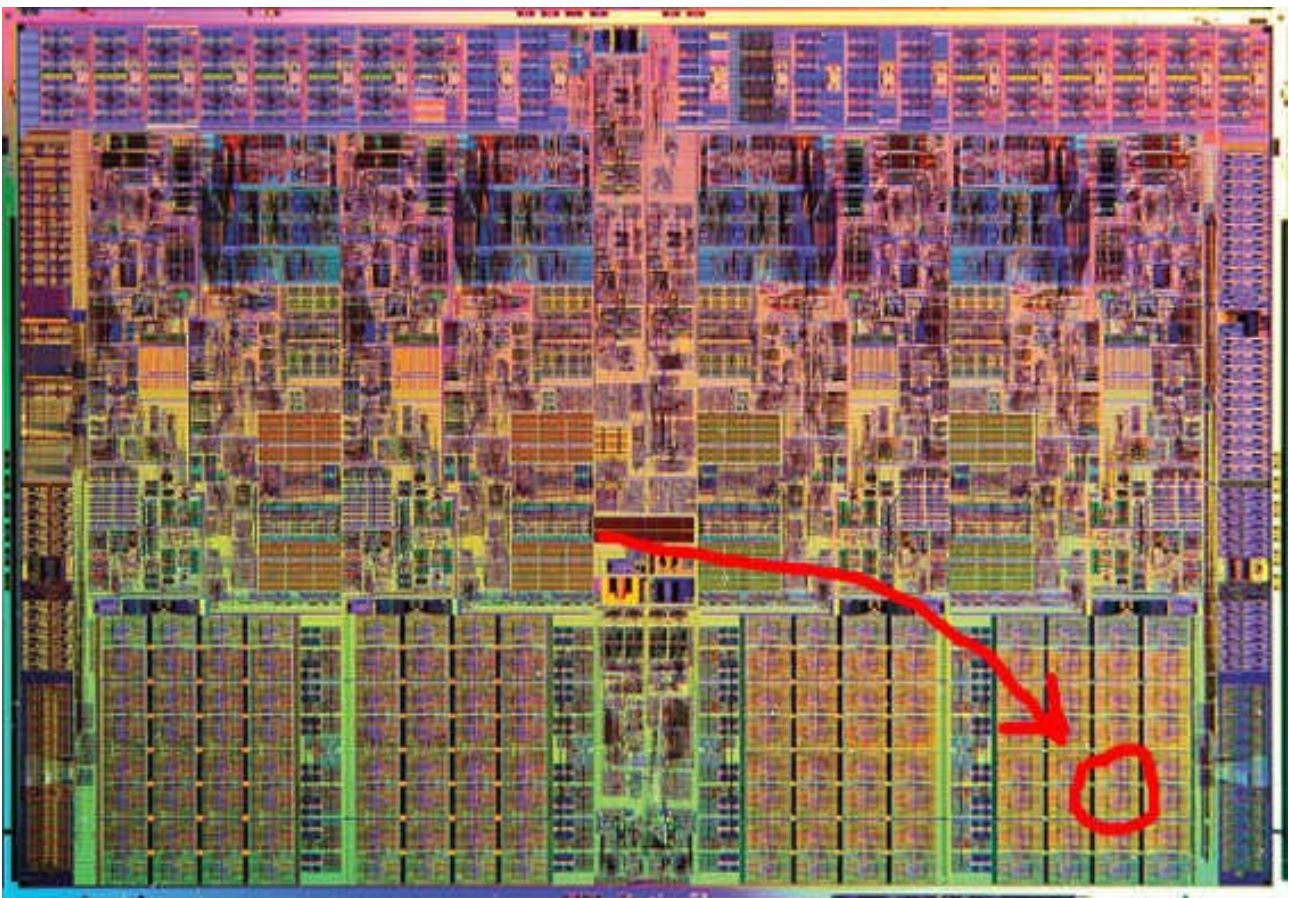
Figure 3:

Chi garantisce al povero Obama che quel gruppetto di transistor non possa essere una funzionalità spionistica cinese, non sradicabile perché incisa nel silicio, e non rintracciabile perché nascosta tra altri 20 milioni di transistor uguali?

Nessuno può farlo, ed Obama lo sa: nascosto dentro quell'integrato montato su un drone armato di missili potrebbe esserci una spia con gli occhi a mandorla pronta a prenderne la guida.

E per concludere, se è preoccupato Obama, che ha la VII flotta e la NSA dalla sua parte, voi non siete preoccupati di quello che fanno le vostre app, quelle che solo perché obbligate dalla legge vi dicono cosa pretendono di sapere?

Ah, già, certo, è perché non avete niente da nascondere.

Originally published at punto-informatico.it.

Nota per che riceve gli articoli via mail. *Medium.com modifica automaticamente i link contenuti negli articoli quando li invia per mail, rendendoli traccianti.* ***La cosa disgusta Cassandra****, che se ne è accorta solo di recente grazie ad una provvidenziale segnalazione. Se ciò superasse il vostro limite di indignazione, ed in attesa che Cassandra trovi una soluzione od un'alternativa, potete fruire dell'articolo direttamente sul sito.*

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 1, 2023.

Canonical link

Exported from Medium on August 27, 2025.